



PATENT ABSTRACTS OF JAPAN

(11) Publication number: 06188828 A

(43) Date of publication of application: 08.07.94

(51) Int. Cl

H04B 7/26
G09C 1/00

(21) Application number: 04267810

(71) Applicant: AMERICAN TELEPH & TELEGR CO <ATT>

(22) Date of filing: 11.09.92

(72) Inventor: REEDS III JAMES ALEXANDER TREVENTI PHILIP A YU I-HSIANG

(30) Priority: 13.09.91 US 91 759314

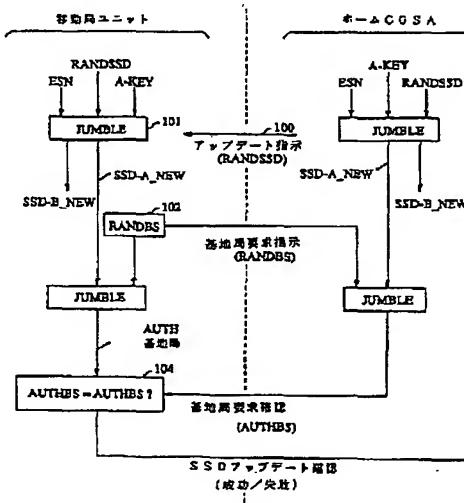
(54) MOBILE STATION AUTHENTICATION METHOD

(57) Abstract:

PURPOSE: To provide a protocol that enciphers a signaling message and can encipher the voice communication and makes a service offerer authenticate a mobile device.

CONSTITUTION: A service offerer assigns only one 'secret' to every mobile device together with other information including the telephone numbers, etc. A command is sent to the mobile device by the request of the service offerer to produce the shared secret data, based on the 'secret'. The shared secret data are produced by means of a bit train that is sent from the service offerer for the relevant purpose. The shared secret data are partly used for encipherment of voices, and this same part or other parts of the secret data are used as the input to a production process of a 2nd enciphering key. This key is used by the mobile device to encipher the control signal produced by the mobile device to affect the property of a call under progression.

COPYRIGHT: (C)1994, JPO



(19)日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11)特許番号

第2589030号

(45)発行日 平成9年(1997)3月12日

(24)登録日 平成8年(1996)12月5日

(51)Int.Cl.⁶
H 0 4 Q 7/38
G 0 9 C 1/00

識別記号
7259-5J

F I
H 0 4 B 7/26
G 0 9 C 1/00

技術表示箇所

(21)出願番号 特願平4-267810

(22)出願日 平成4年(1992)9月11日

(65)公開番号 特開平6-188828

(43)公開日 平成6年(1994)7月8日

(31)優先権主張番号 7 5 9 3 1 4

(32)優先日 1991年9月13日

(33)優先権主張国 米国(US)

(73)特許権者 390035493

エイ・ティ・アンド・ティ・コーポレーション
AT&T CORP.

アメリカ合衆国 10013-2412 ニューヨーク
ニューヨーク アヴェニュー
オブ ジ アメリカズ 32

(72)発明者 ジェームス アレキサンダー リーズ
サード

アメリカ合衆国 07974 ニュージャージー
ニュープロヴィデンス、サウスゲート
ロード 127

(74)代理人 弁理士 三俣 弘文

審査官 関川 正志

最終頁に続く

(54)【発明の名称】 移動局認証方法

1

(57)【特許請求の範囲】

【請求項1】 ホーム局、基地局および移動局からなるシステムにおいて、

ホーム局と移動局が、基地局に知られていないキーコードを、基地局にもらさないように共有するステップと、移動局が、移動局の識別情報と、キーコードおよび付加的データの変換によってキーコードから導出された「共有秘密データ」信号の助けを借りて構成された認証信号とを、基地局に送信するステップと、

基地局でホーム局から受信した「共有秘密データ」の助けを借りて実行された認証信号の評価によって、移動局が送信した認証信号が正当であると判定された場合、基地局と移動局の間に呼を確立するステップとからなることを特徴とする、移動局と基地局の間に呼を確立する前に移動局を認証する方法。

10

2

【請求項2】 キーコードから導出された「共有秘密データ」の助けを借りて構成された前記認証信号が、要素のハッシュ文字列であることを特徴とする請求項1の方法。

【請求項3】 基地局に「共有秘密データ」信号を提供する登録プロトコルをさらに有し、このプロトコルにおいて、

ホーム局は、基地局から、ホーム局に送信された移動局の識別情報およびハッシュ文字列を受信し、

ホーム局は、受信した移動局の識別情報および受信したハッシュ文字列に基づいて、移動局の識別情報を確認し、

ホーム局は、基地局が移動局と通信可能になるように、基地局に「共有秘密データ」信号を送信することを特徴とする請求項2の方法。

【請求項4】 基地局に「共有秘密データ」信号を提供する登録プロトコルをさらに有し、このプロトコルにおいて、

ホーム局は基地局に「共有秘密データ」を送信し、
基地局は、移動局から受信した識別標識およびホーム局から受信した「共有秘密データ」信号に基づいて、移動局の識別情報を確認することを特徴とする請求項2の方法。

【請求項5】 基地局がホーム局に前記確認ステップで取得された結果の表示を送信するステップをさらに有することを特徴とする請求項4の方法。

【請求項6】 ホーム局が基地局に、移動局が「共有秘密データ」の複製を再生することを可能にする種情報を送信するステップをさらに有することを特徴とする請求項2の方法。

【請求項7】 基地局が移動局に、ビットの列および「共有秘密データ」信号の複製を再生する指示を送信するステップと、
移動局が、再生された「共有秘密データ」信号を形成するためにビット列の助けを借りて「共有秘密データ」信号の複製を再生するステップとをさらに有することを特徴とする請求項2の方法。

【請求項8】 前記再生ステップがキーコードを利用するこことを特徴とする請求項7の方法。

【請求項9】 移動局が要求文字列を作成し、その要求文字列を基地局に送信するステップと、

基地局が要求文字列に対する応答を作成し、その応答を移動局に送信するステップと、

移動局がその応答を予想される応答と比較するステップとをさらに有することを特徴とする請求項8の方法。

【請求項10】 基地局に、前記比較ステップの結果の表示を送信するステップをさらに有することを特徴とする請求項9の方法。

【請求項11】 移動局が、再生された「共有秘密データ」信号に関するハッシュ文字列を作成し、そのハッシュ文字列を基地局に送信するステップをさらに有することを特徴とする請求項8の方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、認証プロトコルに関し、特に、セルラ無線電話などの通信の妥当性を保証するためのプロトコルに関する。

【0002】

【従来の技術】 従来の電話においては、各電話セット(ファックス、モ뎀等)は、ローカルセントラルオフィスの交換機の1つのポートに、物理的に接続される。接続は、与えられた電話線あるいは電話線の指定のチャネルを介して行われる。電話線の接続はサービス提供者(通常は通信事業者)によって行われ、従ってサービス提供者は、チャネルの通話が加入者によるものであるこ

とを確信できる。一方、無線電話での加入者の認証は不確かなものである。

【0003】 米国における現在のセルラ電話構成では、加入者が呼び出しを行うと、課金のためそのセルラ電話がサービス提供者に発信者の身元を通知する。この情報は暗号化されていない。第3者がその時点で盗聴すると、加入者の身元情報が得られてしまう。この情報には、加入者の電話番号、加入者の装置の電気シリアル番号(ESN)が含まれている。従って、盗聴者はそのセルラ電話をプログラムして正式な加入者になりすまし、サービスを受けることが可能となる。あるいは、通話中に割り込んで、送信電力を増加させることによって、サービス提供者にある制御コードを送って接続に侵入することもできる。サービス提供者は、接続時およびあるいは通話中の発信者の身元の確認機構を持たないため、このような侵害は基本的に避けられない。

【0004】 盗聴者が身元情報を知ろうとすれば、割当てセル内の全セルラ周波数帯を、自動的に掃引する装置を用いることができる。従って、セルラ電話サービスの侵害を阻止できない。また、音声信号を暗号化していないため、会話の内容を盗聴することができる。つまり、セルラ電話システムにおいて効果的な保護手段が必要とされており、利用者の認証およびプライバシー保護のために、暗号化の利用が必要とされる。

【0005】

【発明が解決しようとする課題】 いくつかの標準的な暗号手法は、セルラ電話等の一般的な認証問題の解決に用いることができるが、実際上の問題もある。まず、プライベートキー暗号アルゴリズムに基づいた、従来の要求/応答プロトコルを用いることができる。この手法では、加入者の移動ステーションに秘密キーが割り当てられ、このキーはホームシステムにも登録されている。提供システムが加入者を認証する場合には、ホームシステムに対して、その加入者の利用に関して照会を行う。ホームシステムは不定期に要求を行い、加入者からのキーを伴う要求に対して、対応する応答を行う機能を果たす。要求および応答は提供システムによって行われ、移動ステーションへの要求も行う。移動ステーションは、要求とその記憶された秘密キーとを処理した結果を応答する。提供システムは、ホームステーションおよび移動ステーションからの応答を比較し、一致した場合に認証されたと見なす。

【0006】 この手法の問題点は、提供システムが発信時の認証の際に、十分早くホームシステムに接続することができず、ホームシステムのデータベースソフトウェアが加入者の秘密キーを調べ、要求/応答ペアを構成することを短期間に行うことができない点である。ネットワークあるいはソフトウェアの数秒の遅延は、加入者が発信する際に、受話器を持ち上げてからダイヤルトーンが聞こえるまでのデッドタイムを増し、さらに(セルラ

40

提供者の現在用いている制御ネットワークおよび交換装置によって) 遅延時間が増す。現状では、そのような遅延は許容されない。

【0007】パブリックキー暗号システムは、認証問題を解決するもう一つの標準的な手法である。一般的に、各移動ステーションはサービス提供者のパブリックキーによって、“パブリックキー証書”が与えられ、その移動ステーションがサービス提供者の合法的な利用者であることを示す。さらに、各移動局に秘密データ(プライベートキー)が与えられ、証書と同時に第3者に合法的な利用者であることを示すのに用いられる。

【0008】例として、サービス提供者はRSAキーペア(F, G)を、Fをプライベート、Gをパブリックとして有する。サービス提供者は各移動局に、そのRSAキーの独自のペア(D, E)を、F(E)(提供者のプライベートキーFを用いて移動局のパブリックキーEを暗号化したもの)と共に与える。移動局は、提供システムに、(E, F(E))を送ることによってその身元を提示する。提供システムでは、F(E)にGを用いてEを得る。提供システムは要求Xを生成し、移動局のパブリックキーEを用いて暗号化してE(X)を得て、それを移動局へ送る。移動局は、E(X)にプライベートキーDを用いてXを得て、解読した状態でそれを応答として提供システムへ返送する。

【0009】この問題について、処理あるいはデータ伝送量を減少させる改良例もあるが、セルラ電話で現在用いられているハードウェアにおいて、数秒以下で効率的に実行できる、パブリックキー認証手法は存在しない。認証時には、提供システムとホームシステム間でのネットワークの接続性は必要とされないが、従来手法での時間的な制限が問題となるように、パブリックキー手法でも同様の制約が生じる。

【0010】

【課題を解決するための手段】セルラ電話技術のセキュリティ需要は、共有秘密データフィールドによる配置によって満たされる。移動局ユニットは、サービス提供者によってそれに割り当てられた秘密を保持し、その秘密から共有秘密データフィールドを生成する。サービス提供者もその共有秘密データフィールドを生成する。移動局ユニットが基地局のセルに入ると、自分自身を基地局に認知させ、ハッシュ認証文字列を基地局に与える。基地局は提供者に問い合わせ、その移動局ユニットが正当な装置であると判定された場合、提供者は基地局に共有秘密データフィールドを提供する。その後、移動局ユニットは、共有秘密データフィールドを使用して、移動局ユニットと基地局の間で実行される認証プロセスの助けを借りて、基地局と通信する。

【0010】この配置の1つの特徴は、異なる基地局は、提供者によって移動局ユニットに組み込まれた秘密へのアクセス許可を有しないことである。また、移動局

ユニットとの対話に成功した基地局のみが共有秘密データフィールドを有する。また、その数は、提供者が、単に、新たな共有秘密データフィールドを作成するよう移動局ユニットに指示することにより、制限することができる。

【0011】この配置のもう1つの特徴は、より多くの時間がかかる、秘密を使用する認証プロセスは、提供者が関わる場合にのみ起こるが、これは、移動局ユニットが最初にセルに入るとき(または共有秘密データフィールドが損傷を受けた疑いがあるとき)であり、頻繁には起こらない。

【0012】呼の発信、呼の着信、およびその他の機能は、本質的に同一の認証プロトコルおよび同一のハッシュ関数を使用して認証される。ハッシュされる情報に若干の相違が現れる。

【0013】

【実施例】移動セルラ電話システムでは、多数の移動電話、少数のセルラ無線提供者(各提供者が複数の基地局を有する)、複数の交換ネットワーク提供者(通信事業者)から構成される。セルラ無線提供者と通信事業者は、セルラ電話加入者によって、セルラおよび非セルラ両者の電話加入者との通話を可能にするように組合せられる。図1に概略の構成を示すように、通信事業者IおよびIIは、交換機10-14を有する交換ネットワークを形成して結合される。固定局ユニット20および21は交換機10に接続され、移動局ユニット22および23は不特定位置で、基地局30-40は交換機10-14に接続される。基地局30-34は提供者1、基地局35および36は提供者2、基地局37は提供者4、基地局38-40は提供者3にそれぞれ属する。本発明の目的では、基地局は複数の送信器を有するセルと同じ意味である。セルの集合体は、図1の基地局30、31および32のように、地理上のセルラサービスエリア(CGSA)を形成する。

【0014】各移動局ユニットは、そのユニット固有の電気シリアル番号(ESN)を有する。ESN番号はユニットの製造時に、製造者によって割り当てられ(例えば、ROM内に)、アクセスはできるが変更はできない。

【0015】利用者がその移動電話ユニットのサービスアカウントを申請すると、サービス提供者は利用者に、電話番号(MIN1指定)、エリアコード(MIN2指定)、“秘密キー”(Aキー)を割り当てる。MIN1およびMIN2指定は提供者のCGSAに関連し、図1の構成の全基地局は、特定のMIN2およびMIN1ペアの属するCGSAを識別することができる。Aキーは、利用者装置および提供者のCGSAプロセッサ(図1には示さず)だけが知っている。CGSAプロセッサは、ユニットのESN、Aキー、MIN1およびMIN2指定の他、サービス提供者の必要な情報を保持してい

る。

【0016】MIN1指定およびAキーがインストールされ、CGSAプロセッサが、移動局ユニットに特定のランダムシーケンス(RANDSSD)を送信し、“共有秘密データ”(SSD)の作成を指示することによって、利用者のユニットが初期化される。CGSAは、RANDSSDおよびSSDフィールドの生成を、移動局ユニットの存在するセルの基地局を通して送信する。SSDフィールドの作成は図2に示されるプロトコルに従う。

【0017】図1の構成では、各基地局は、あらかじめ割り当てられたチャネルのいくつかを用いて、そのセル内の全てのユニットに情報を送信する(送信バンド)。さらに、各移動局ユニットに対して、相互に確認した、(一時的に)割り当てられたチャネルによって、双方向通信を確保する。基地局と移動局ユニットで、通信チャネルの確認を行う手法は、本発明には重要でないため、ここでは詳しく述べない。例としては、移動局ユニットが全チャネルをスキャンし開きチャネルを選択する手法が考えられる。その後基地局へ、そのMIN2およびMIN1指定を送信し(元テキストあるいはパブリックキーによって暗号化されたもののいづれか)、基地局に認証プロセスの開始を許可する。認証通信が確立されると、基地局は移動局を他のチャネルへスイッチしても良い。

【0018】本発明による移動電話システムでの呼び出しの確立と保持手法では、認証プロセスは会話中に多数回行われる。従って、認証プロセスは比較的安全で簡単に行うことができる。設計を簡単に導入費用を抑えるために、移動局ユニットおよび基地局の両方で同じプロセスを用いるべきである。

【0019】多くの認証プロセスは、プロセスを行うために、ハッシング機能あるいは一方向機能を用いる。ハッシング機能は、“秘密キー”をサインに変換する、多対一のマッピングを実行する。以下に、簡単で、速く、効果的で、柔軟性のあるハッシング機能の一例を示す。これは、本発明の認証プロセスに好都合であるが、他のハッシング機能を用いることもできる。

【0020】ジャンブルプロセス
ジャンブルプロセスでは、dの“秘密”データワードb(i)の“サイン”を、kワードのキーx(j)によって生成する。ここで、d, i, j, およびkは整数である。“サイン”的生成プロセスは、1回に一つのデータワードを実行する。この説明のために、ジャンブルプロセスで操作するワードが8ビット長(0~255の範囲を与える)であるとするが、他のワードサイズでも実行できる。“秘密”データブロック長を、鋸歯状波関数に用いて、

$$s_d(t) = t \quad 0 \leq t \leq d-1$$

$$s_d(t) = 2d-2-t \quad d \leq t \leq 2d-3$$

$$s_d(t) = s_d(t+2d-2) \quad (\text{全 } t \text{ に対して})$$

とする。この関数は、z=0およびi=0から始め、0≤6d-5の範囲で連続的に増加する整数iに対する以下のプロセスで用いられる。

a) b(s_d(i))を、b(s_d(i))b(s_d(i)+x(i_k)+SBOX(z) mod 256によってアップデートし、ここで、i_kはi mod k, SBOX(z)=y+[y/2048] mod 256, y=(z(+16)(z+111)(z)とし、[y/2048]はyを2048で割った整数部を示し、(+)はビット排他OR関数である；
b) zを、z=z+b(s_d(i)) mod 256によってアップデートする。

【0021】上記のプロセスでは、データとキーの間に明確な区別は無いことが分かる。従って、認証に用いられるどの符号列も、上記のプロセスでキーとして用いられる部分を有することができる。逆に、キーと結合されたデータワードは、“認証”符号列と考えられる。各ワードb(i)は、0≤i<d-1で1回に一つそれぞれ分割され、ハッシングを“適切”に行うことができる。ハッシングプロセス自体には、余分のバッファは必要とされない。

【0022】上述のプロセスで必要とされる操作は、シフト(2048による割り算)、切捨て(□関数およびmod 256関数)、加算、乗算、およびビット排他OR関数であるため、基本的な従来のプロセッサで簡単に実行できる。

【0023】図2のSSDフィールドの初期プロセスに戻って、RANDSSDシーケンスおよび新規のSSDフィールド(図2の矢印)の作成指示が移動ステーションで受信されると、図4に従って新規のSSDフィールドが生成される。移動局ユニットは、ESN指定、Aキー、RANDSSDシーケンスを結合して認証符号列を形成する。認証符号列はジャンブルブロック101(前述)へ導かれ、SSDフィールドを出力する。SSDフィールドは2つのサブフィールドから構成される：認証手順の補助に用いられるSSD-Aサブフィールド、および音声プライバシー手順およびある信号メッセージ(後述)の暗号化を補助に用いられるSSD-Bサブフィールドである。注意すべき点は、上記のようにして形成されたSSDフィールドを再分割することによって、または、最初にSSDフィールドを拡張することによって、さらに多くのSSDサブフィールドを作成することも可能であることがある。SSDフィールド内のビット数を増大させるには、より多くのデータビットから開始するだけでよい。以下に述べるように、これは通常必要とされることはない。

【0024】ホームCGSAプロセッサは、受信されたMIN2およびMIN1指定の割り当てられた移動局ユニットのESNおよびAキーを知っている。また、送信

したRANDSSDシーケンスも知っている。従って、ホームCGSAプロセッサでは、移動局ユニットのSSDフィールド生成プロセスを複製する。RANDSSD信号を、ESN指定およびAキー、前述のジャンブルプロセスと結合することによって、CGSAプロセッサは新規のSSDフィールドを生成し、それをSSD-AおよびSSD-Bのサブフィールドに分割する。しかし、ホームプロセッサで生成されたSSDフィールドは検証されねばならない。

【0025】図2のように、SSDフィールドの検証は移動局ユニットによって行われる。移動局ユニットはブロック102においてランダム要求シーケンス(RANDBSシーケンス)を生成し、サーバ基地局(移動局ユニットが位置するエリアをサービスする基地局)を通じてホームCGSAプロセッサへそれを送信する。図5のように、ホームCGSAプロセッサは、要求RANDBSシーケンス、移動局ユニットのESN、MIN1指定、新規生成されたSSD-Aを結合し、ジャンブルプロセスで用いられる認証符号列を形成する。この例では、ジャンブルプロセスは、移動局へ送られる分割された認証信号AUTHBSを生成する。移動局はまた、RANDBSシーケンス、ESN指定、MIN1指定、新規生成されたSSD-Aを結合し、ジャンブルプロセスで用いられる認証符号列を形成する。移動局は、そのジャンブルプロセスの結果と、ホームCGSAプロセッサからの分割された認証信号(AUTHBS)とを比較する。比較ステップ(ブロック104)で一致すると、移動局は、SSDフィールドのアップデートに成功したことと示す確認メッセージを、ホームCGSAプロセッサへ送る。一致しない場合には、その比較結果を移動局が送信する。

【0026】移動局が初期化されても、SSDフィールドは、ホームCGSAプロセッサが新規のSSDフィールドを生成することを指示するまで、そのまま保持される。これは例えば、SSDフィールドが処理されたことが認められる場合に生じる。そのような場合、ホームCGSAプロセッサは移動局にもう一つのRANDSSDシーケンスを送り、新規のSSDフィールドを生成するように指示する。

【0027】前述のように、セルラ電話では各基地局から、そのセル内の全ての移動局ユニットのために、種々の情報信号が送信される。図1の構成では、基地局から送信される信号の一つは、ランダムあるいは疑似ランダムシーケンス(RANDシーケンス)である。RANDシーケンスは、移動局ユニットで生成および送信された信号をランダム化して、種々の認証プロセスに用いられる。RANDシーケンスは、録音/再生による妨害を防ぐために定期的に変更されねばならない。RAND信号の待ち時間の設定手法として、予想される平均呼び出し時間より短く設定する方法がある。従って、通常移動局

では、連続する呼び出しに対して異なったRAND信号を用いることになる。

【0028】本発明の1つの目的によれば、移動局ユニットは、セルに入ったことを検知するとすぐに認証可能なように基地局に登録する。移動局ユニットは、認証された場合にのみ、通話を開始すること、または、基地局に対して移動局ユニットへの通話を指示することができる。

【0029】移動局ユニットは、登録プロセスを開始すると、基地局によって同報されたRANDシーケンスを受信し、そのMIN1およびMIN2指定ならびにそのESNシーケンス(平文で)を、ハッシュ認証文字列とともに送信する。図6に従って、ハッシュ認証文字列は、RANDシーケンス、ESNシーケンス、MIN1指定およびSSD-Aサブフィールドを連結して認証文字列を形成し、その認証文字列をジャンブルプロセスに送ることによって導出される。ジャンブルプロセスの出力のハッシュ認証文字列は、ESNシーケンスとともにサーバ基地局に送られる。

【0030】ある実施例では、移動局ユニットによって使用されるRANDシーケンスの全部または一部が(ESNシーケンスならびにMIN1およびMIN2指定とともに)サーバ基地局にも送られる。その理由は、ハッシュ認証文字列が基地局に到達するときまでにRAND値が変化する可能性があるためである。

【0031】基地局側では、サーバ基地局は、RANDシーケンスを知っており(基地局がそれを作成したため)、また、移動局ユニットが確認したESNならびにMIN2およびMIN1指定をも知っている。しかし、サーバ基地局は、移動局ユニットのSSDフィールドは知らない。それが(MIN1およびMIN2指定から)知っているのは、移動局ユニットのホームCGSAプロセッサの識別情報である。

【0032】その結果、認証プロセスは、移動局ユニットのホームCGSAプロセッサへ、MIN1指定、ESNシーケンス、移動局ユニットが作成し送信したハッシュ認証文字列、およびサーバ基地局が同報した(そして、移動局ユニットが、作成したハッシュ認証文字列に組み込んだ)RANDシーケンスを送ることによって進行する。移動局ユニットのMIN1指定およびESNシーケンスから、ホームCGSAプロセッサは、移動局ユニットの識別情報、およびそれによって、移動局ユニットのSSD-Aサブフィールドを知る。

【0033】従って、移動局ユニットがしたのと同じように認証文字列を作成し、それをジャンブルプロセス(図6)に送ることができる。移動局ユニットのホームCGSAプロセッサによって作成されたハッシュ認証文字列が、移動局ユニットで作成されサーバ基地局によって提供されたハッシュ認証文字列と一致した場合、確認は成功と認められる。このような場合、ホームCGSA

プロセッサはサーバ基地局にその装置のSSDフィールドを提供する。ちなみに、ESN指定およびSSDフィールドを安全に保持するため、基地局とCGSAプロセッサの間の通信は暗号化形式で実行される。

【0034】上記のプロトコルでは、移動局ユニットのCGSAプロセッサは、ハッシュ認証文字列の正当性の確認を試みる。確認が失敗した場合、CGSAプロセッサは、サーバ基地局に対し、移動局ユニットは認証されなかったことを通知し、移動局ユニットとの接触が放棄されるか、または、移動局ユニットに登録プロセスの再試行が指示されるべきであることを提案する。登録プロセスを再試行するためには、ホームCGSAプロセッサは、認証プロセスへの関与を続行するか、または、それをサーバ基地局に委任することができる。

【0035】後者の場合、サーバ基地局はホームCGSAプロセッサに対し移動局ユニットのESNシーケンスおよびMIN1指定を通知し、CGSAプロセッサは移動局ユニットのSSDフィールドおよびSSDフィールドの作成に使用されたRANDSSDを応答する。ハッシュ認証文字列を作成し、それを移動局ユニットによって送信されたハッシュ認証文字列と比較するという意味で、認証がサーバ基地局によって実行される。続いて、ホームCGSAプロセスがサーバ局によって移動局ユニットにRANDSSDを送信することなしに再試行指令が実行可能である。この「登録」プロトコルを図3に示す。

【0036】移動局ユニットが（上記のプロセスによって）サーバ基地局に「登録」されると、サーバ基地局は移動局ユニットのESNおよびSSDフィールドを所有し、そのセルでの以後の認証プロセスは、次の1つの場合を除いてホームCGSAプロセッサの参照なしにサーバ基地局で実行可能である。何らかの理由で、SSDフィールドを変更したい場合には、通信はホームCGSAプロセッサと移動局ユニットの間で有効であり、サーバ基地局はこの通信のための通路としてのみ作用する。その理由は、新たなSSDフィールドの作成は秘密Aキーへのアクセスを必要とし、CGSAプロセッサによるAキーへのアクセスは全く許されていないためである。

【0037】従って、新たなSSDフィールドが作成され移動局ユニットがホームCGSAのエリアに存在しない場合、次のことが起こる。

- ・ ホームCGSAプロセッサはRANDSSDシーケンスを作成し、そのRANDSSDシーケンスに基づいてSSDフィールドを変更する。
- ・ ホームCGSAプロセッサはサーバ基地局にRANDSSDシーケンスおよび新たに作成されたSSDフィールドを提供する。
- ・ サーバ基地局は、移動局ユニットに対し、そのSSDフィールドを変更するよう指示し、移動局ユニットにRANDSSDシーケンスを提供する。

・ 移動局ユニットはSSDフィールドを変更し、サーバ基地局に要求を送る。

・ サーバ基地局は（上記の）AUTHS文字列を作成し、それを移動局ユニットに送る。

・ 移動局ユニットはAUTHS文字列を確認し、サーバ基地局に対し、移動局ユニットおよびサーバ基地局の両方が同一のSSDフィールドを有することを通知する。

【0038】サーバ基地局によって登録された後、移動

10 局ユニットは図7の認証プロセスとともに通話を開始することができる。通話開始シーケンスは、信号RAND、ESN、SSD-Aおよび少なくともいくつかの被呼者識別（電話）番号（図7のMIN3）を連結する。連結された信号は、サーバ基地局によって確認可能なハッシュ認証シーケンスを生成するためにジャンブルプロセスに送られる。もちろん、サーバ基地局での確認を可能にするためには、被呼者識別情報（および、以前のように、おそらくRAND信号の一部）は基地局によって受信可能な方法（例えば平文）で送信されなければならない。認証シーケンスが確認されると、基地局は通話を処理し被呼者への接続を形成することが可能となる。

【0039】移動局ユニットが「被呼者」である場合に移動局ユニットに接続するためのプロトコルは図6の登録プロトコルに従う。すなわち、サーバ基地局は、被呼移動局に対し、RANDシーケンス、ESN指定、MIN1指定およびSSD-Aサブフィールドから作成された認証シーケンスを送信することを要求する。認証が実行されると、基地局と被呼者移動局ユニットの間には、被呼者移動局ユニットが、通話を発信した移動局ユニット（または固定装置）から発信されたデータを受信し、それにデータを送信するためのバスが設定される。

【0040】上記のすべての認証は、認証されるパケットすなわち文字列自体に関するのみ（確認されるという意味で）有効であることに注意すべきである。その他の場合にセキュリティを強化するためには、3つの異なる付加的なセキュリティ手段が使用可能である。それらは、音声暗号化、臨時の再認証、および制御メッセージ暗号化である。

【0041】【音声暗号化】音声信号は、最初にそれを40 デジタル形式に変換することによって暗号化される。これはさまざまな従来の方法で実現可能であり、圧縮や誤り訂正符号を加えることもできる。デジタル信号のビットはKビットからなる連続するグループに分割され、各グループが暗号化される。特に、移動局ユニットおよび基地局の両方において、RANDシーケンス、ESNおよびMIN1指定、ならびにSSD-Bサブフィールドは連結されジャンブルプロセスに送られる。

【0042】ジャンブルプロセスは2Kビットを生成し、これらのビットはそれぞれKビットからなるグループAおよびBに分割される。移動局ユニットでは、グル

ープAが出力音声を暗号化するために使用され、グループBが入力音声を解読するために使用される。逆に、基地局では、グループAが入力音声を解読するために使用され、グループBが出力音声を暗号化するために使用される。図8はこの音声暗号化および解読プロセスを示す。

【0043】[再認証] 基地局の希望により、基地局によってアクティブであると信じられている移動局ユニットが、実際に、アクティブであると認定された移動局ユニットであることを確認するために、再認証プロセスが開始される。これは、基地局によって、移動局ユニットに対し、図9に従ってハッシュ認証シーケンスの送信を要求することによって実現される。このような各要求とともに、基地局は特殊な(RANDU)シーケンスを送信する。移動局ユニットは、RANDUシーケンス、移動局ユニットのエリアコードMIN2指定、MIN1指定およびSSD-A指定を連結することによってハッシュ認証シーケンスを作成する。連結された文字列はジャンブルプロセスに送られ、生じたハッシュ認証文字列が基地局に送られる。基地局は、この時点で、ハッシュ認証文字列が正当であることを確認することができる位置にある。

【0044】[制御メッセージ暗号化システム] 第3のセキュリティ手段は、制御メッセージのプライバシーの保証を取り扱う。設定された通話の間に、制御メッセージの送信を要求するさまざまな状況が生じることがある。ある場合は、制御メッセージは通話を発信した移動局または基地局に重大な悪影響を与えることがある。このため、対話の進行中に送信されるある種の制御メッセージを(十分に)暗号化することが所望される。あるいは、選択されたメッセージ種の選択されたフィールドを暗号化することも可能である。これは、クレジットカード番号のような「データ」制御メッセージや、通話再定義制御メッセージを含む。これは制御メッセージ暗号化システムによって実現される。

【0045】制御メッセージ暗号化システム(CMC)は以下の性質を有する対称鍵暗号化システムである。

- 1) 比較的安全である。
- 2) 8ビットコンピュータ上で効率的に動作する。
- 3) 自己反転的である。

【0046】CMCの暗号鍵は、次のようにして「秘密」(例えば、SSD-Bサブフィールド)から導出される、256ビットの配列TBOX[z]である。

1. $0 \leq z < 256$ の範囲の各zに対し、 $TBOX[z] = z$ とおく。
2. 配列TBOX[z]および秘密(SSD-B)をジャンブルプロセスに送る。

これは、本質的に、(図8のビット数が256ビットではなく2Kビットであることを除いては)図8の要素301、302および303で示されたものである。

【0047】鍵が導出されると、CMCが、制御メッセージを暗号化および解読するために使用可能となる。あるいは、鍵が使用されるたびごとに、鍵を「大急ぎで」導出することも可能である。CMCは複数バイトの可変長メッセージを暗号化する能力を有する。CMCの操作は自己反転的、あるいは逆数的である。すなわち、平文を生じるために暗号文に対してなされる操作と、暗号文を生じるために平文に対してなされる操作が、完全に同一である。従って、CMC操作を2度実行すると、データは不变のままである。

【0048】以下の説明では、暗号化プロセス(および解読プロセス)に対し、平文(または暗号文)はデータバッファ内に存在し、CMCは、そのデータバッファの内容に対し、データバッファの最終内容が暗号文(または平文)を構成するように作用する、と仮定する。これは、図10の要素502および504が1つの同一のレジスタでよいことを意味する。

【0049】CMCは3つの連続する段階からなり、それぞれデータバッファ内の各バイト列を変更する。データバッファの長さががdバイトであり、各バイトをb(i)で表すとき、 $0 \leq i < d$ の範囲のiに対し、

I. CMCの第1段階は次の通りである。

1. 変数zを0に初期化する。
2. $0 \leq i < d$ の範囲の連続する整数値iに対し、
 - a. 変数qを、 $q = z \# (i \text{の下位バイト})$ によって形成する。ただし、#はビットごとのブール排他的OR演算子である。
 - b. 変数kを、 $k = TBOX[q]$ によって形成する。
 - c. $b(i)$ を、 $b(i) = b(i) + k \bmod 256$ と更新する。
 - d. zを、 $z = b(i) + z \bmod 256$ と更新する。

30 I I. CMCの第2段階は、次の通りである。

1. $0 \leq i < (d-1)/2$ の範囲のiのすべての値に対し、 $b(i) = b(i) \# (b(d-1-i) \text{ OR } 1)$ とする。ただし、ORはビットごとのブールOR演算子である。

40 I I I. CMCの最終段階は、第1段階の逆である解読である。

1. 変数zを0に初期化する。
2. $0 \leq i < d$ の範囲の連続する整数値iに対し、
 - a. 変数qを、 $q = z \# (i \text{の下位バイト})$ によって形成する。
 - b. 変数kを、 $k = TBOX[q]$ によって形成する。
 - c. zを、 $z = b(i) + z \bmod 256$ と更新する。
 - d. $b(i)$ を、 $b(i) = b(i) - k \bmod$

256 と更新する。

【0051】選択された制御およびデータメッセージを暗号化および解読するために使用されるこれら3段階のプロセスを図10に示す。1つの所望される実施例では、第1段階および第3段階はそれぞれ自己鍵暗号化および解読である。自己鍵系は、系の出力が以後の系の出力に作用するために使用されるような時間変動系である。暗号および自己鍵系に関するこれ以上のことは、W. ディフィー、M. E. ヘルマン著「プライバシーと認証：暗号入門」I. E. E. E. 会議録第67巻第3号（1979年3月）を参照。

【0052】【移動局ユニット機器】図11は、移動局ユニットハードウェアのブロック図である。これは、セルラ電話のキーパッド、受話器および装置の電源制御スイッチ（図示せず）を含む制御ブロック200を有する。制御ブロック200はプロセッサ210に接続される。プロセッサ210は、音声信号をデジタル表現に変換すること、誤り訂正符号を組み込むこと、出力デジタル音声信号を暗号化すること、入力音声信号を解読すること、さまざまな制御メッセージを形成および暗号化（さらに解読）すること、などのような、移動局ユニットの動作を制御する。

【0053】ブロック210は、信号の送受信に関連する回路の集合からなるブロック220に結合される。ブロック200～220は、市販の移動電話装置によって現在実行されている機能を実行する（市販の装置は暗号化および解読は実行しないが）、基本的には従来のブロックである。これまで説明した認証および暗号化プロセスを実現するため、図11の装置は、プロセッサ210に結合したいくつかのレジスタからなるブロック240と、同じくプロセッサ210に結合した「個性」モジュール230をも含む。モジュール230は、移動電話装置の物理的構造の一部でもよいし、ソケットインターフェースを通じて移動電話装置に結合した取り外し可能（かつはめ込み可能）なモジュールでもよい。これは、電磁パスすなわち接続を通じてプロセッサ210に結合してもよい。要するに、モジュール230は、例えば、「スマートカード」である。

【0054】モジュール230はジャンブルプロセッサ231およびプロセッサ231に付随するいくつかのレジスタからなる。あるいは、他の所望される実施例では、Aキーのみがモジュール230内に存在する。Aキー、ならびにMIN1およびMIN2指定を、ブロック240のレジスタではなく、モジュール230のレジスタに組み込む（そして保持する）ことからいくつかの利益が生じる。

【0055】生成されたSSDフィールドをモジュール230のレジスタに格納することも有益である。さらに、プロセッサ231のプロセスを実行するために必要な作業レジスタをモジュール230のレジスタに含める

ことも有益である。これらの要素をモジュール230に含めることにより、ユーザは、それを異なる移動局ユニット（例えば「拡張」移動局ユニット）で使用し、重要な情報がモジュール外に格納されることないようにするために、モジュールを携帯することができる。もちろん、移動局ユニットは、モジュール230が装置の統合的かつ永続的部分であるように生産することも可能である。このような実施例では、ジャンブルプロセッサ231はプロセッサ210内に合併することができる。ブロック240は、装置のESN指定および受信されるさまざまなRANDシーケンスを格納する。

【0056】上記の説明はセルラ電話環境における加入者認証について述べられており、携帯用ポケット受話器に使用される個人通信ネットワークを含むものであるが、本発明の原理は、通信が十分に安全ではないと認識され、模写が潜在的問題であるような他の状況における利用可能性を有することは明らかである。これには例えばコンピュータネットワークが含まれる。

【0057】

20 【発明の効果】以上述べたごとく、本発明によれば、現在セルラ電話で使用される種類のハードウェアを使用して、高速で効率的に実行可能な公開鍵認証方式が与えられる。

【図面の簡単な説明】

【図1】固定および移動電話の両方のサービスのために相互接続された、ネットワーク提供者およびセルラ無線提供者の構成を示す図である。

【図2】共有秘密データフィールドの作成と同一性の検証を行うプロセスを示す図である。

30 【図3】例えば移動局ユニットが最初に基地局によってサービスされるセルに入った場合の、訪問先の基地局における登録プロセスを示す図である。

【図4】共有秘密データを作成するために連結されハッシュされた要素を示す図である。

【図5】確認シーケンスを作成するために連結されハッシュされた要素を示す図である。

【図6】移動局ユニットが発信する際に、登録シーケンスを作成するために連結されハッシュされた要素を示す図である。

40 【図7】呼開始シーケンスを作成するために連結されハッシュされた要素を示す図である。

【図8】移動局ユニットにおける音声暗号化および解読のプロセスを示す図である。

【図9】再認証シーケンスを作成するために連結されハッシュされた要素を示す図である。

【図10】選択された制御およびデータメッセージを暗号化および解読するための3段プロセスを示す図である。

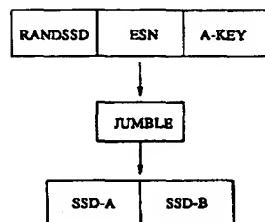
50 【図11】移動局ユニットのハードウェアのブロック図である。

【符号の説明】

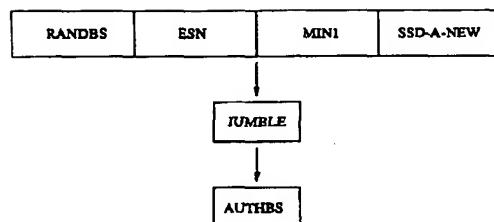
10-14 交換機
20-21 固定局
22-23 移動局
30-40 基地局
101 ジャンブルブロック
102 ブロック
104 ブロック
200 制御ブロック

210 プロセッサ
220 ブロック
230 モジュール
231 プロセッサ
240 ブロック
301-303 要素
502 要素
504 要素

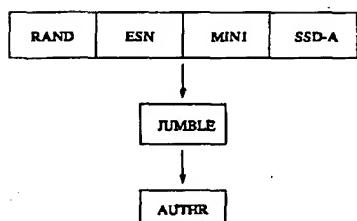
【図4】



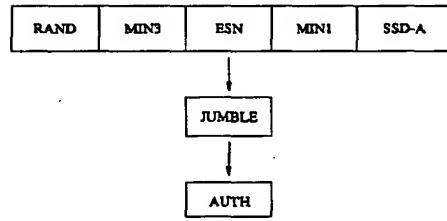
【図5】



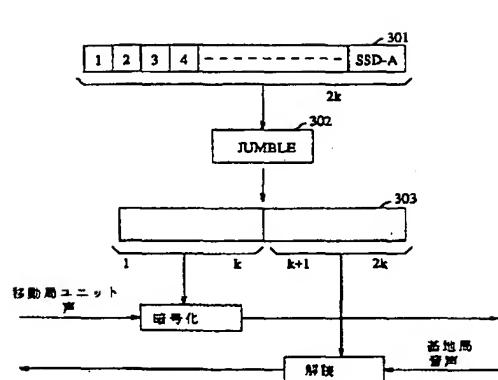
【図6】



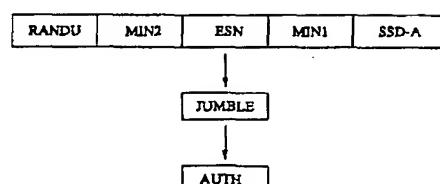
【図7】



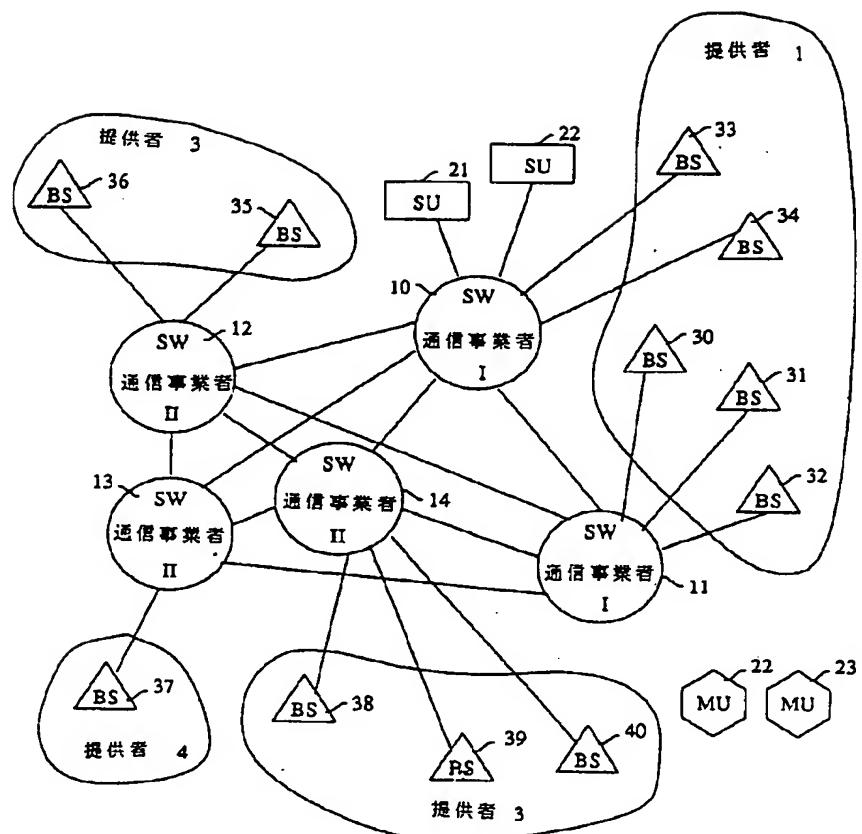
【図8】



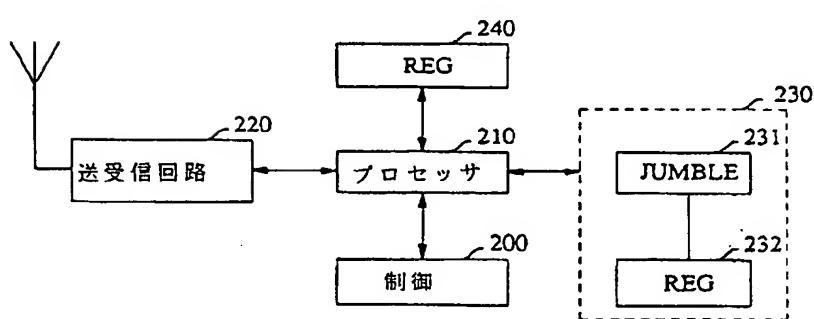
【図9】



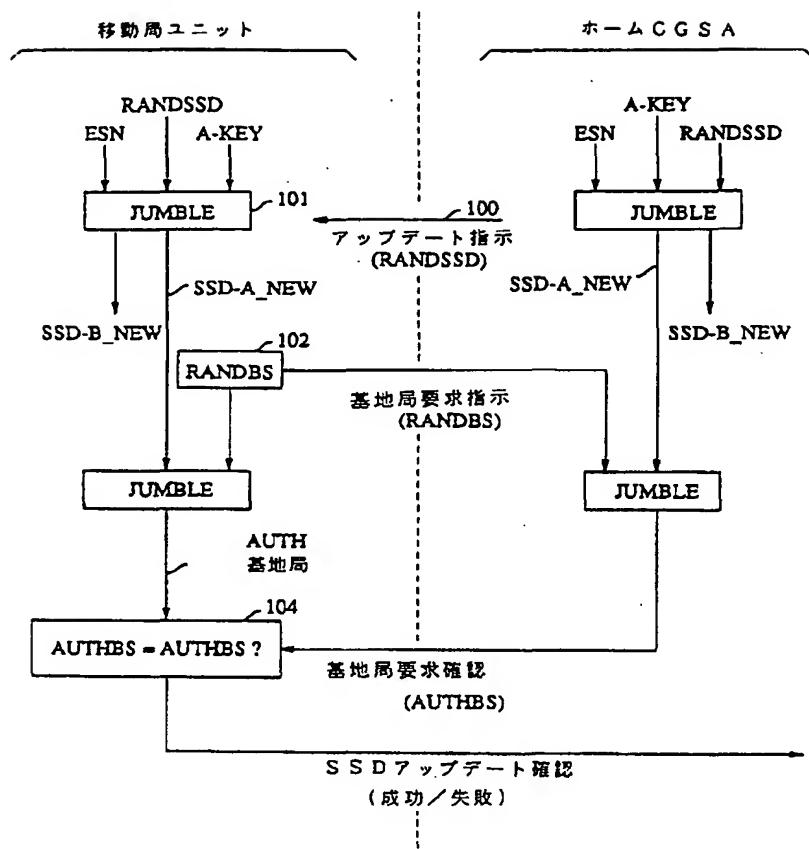
【図1】



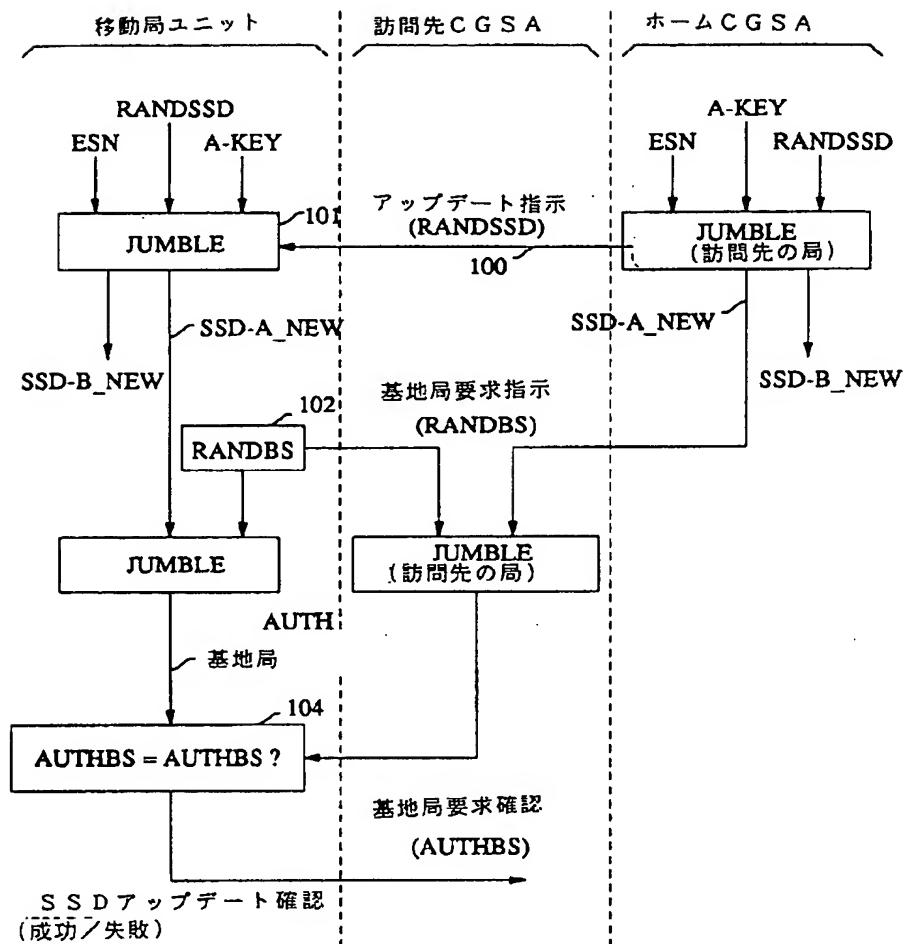
【図1-1】



【図2】

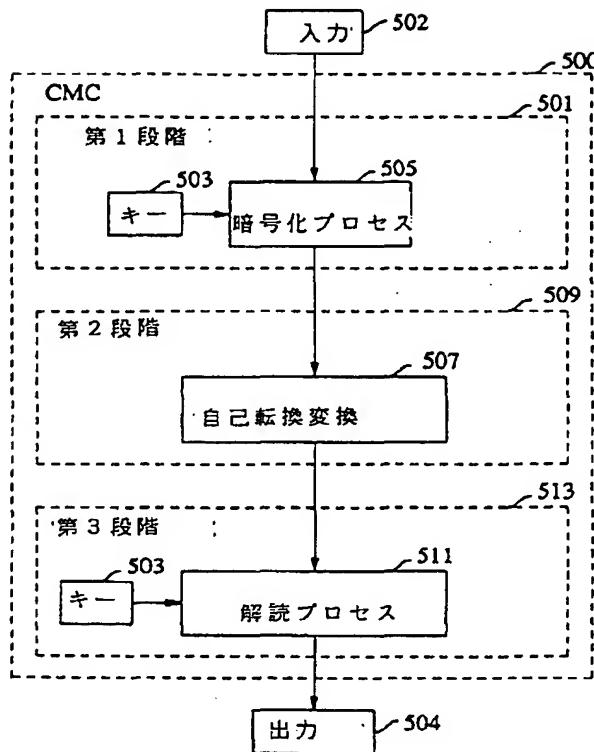


【図3】



【図10】

制御メッセージ暗号化システム



フロントページの続き

(72)発明者 フィリップ アンドリュー トラヴァン
ティ
アメリカ合衆国 07974 ニュージャー
ジー マーレー ヒル、キャンドルウッ
ド ドライヴ 15

(72)発明者 イーシアン ユ
アメリカ合衆国 07927 ニュージャー
ジー シーダーノールズ、ヒッコリープ
レース 9

(56)参考文献
特開 昭63-48930 (J P, A)
特開 平1-307341 (J P, A)
特開 平3-203431 (J P, A)
特開 平1-164139 (J P, A)
特開 昭62-278869 (J P, A)
特開 平3-69220 (J P, A)
米国特許4555805 (U S, A)
米国特許4157454 (U S, A)
米国特許5303285 (U S, A)